REMARKS

The Examiner rejected claim 1 as being obvious over Pichlmaier in view of Windows NT as illustrated by the patent to Ozzie and the article to Hadfield. Claim 1 is a method of performing a password-protected secure function that protects a user's password from inadvertent or unintentional disclosure to a foreign party. Particularly, claim 1 authenticates password entry screens to the user by including authentication indicia on the password entry screen when it is displayed to the user. The authentication indicia functions as a "reverse password" for the user. A valid password entry screen would always contain the authentication indicia (i.e., the reverse password), while an invalid password entry screen would not. Thus, the mere presence or absence of the authentication indicia from the password entry screen allows the user to instantly differentiate a valid password entry screen from an invalid or "spoofed" password entry screen.

Pichlmaier, the primary reference, fails to teach or suggest claim 1 for several reasons. First, Pichlmaier discloses a validation process that operates in a vastly different manner than does the claimed authentication method. Rather than authenticate a password entry screen to a user, Pichlmaier discloses a <u>data exchange</u> method that uses encoded data words communicated over a network to <u>mutually validate remotely located computers</u>. *Pichlmaier*, col. 2, ll. 17-21. In other words, the object of the Pichlmaier validation process is to validate the entire computer system. If authentication is successful (i.e., the system is valid), Pichlmaier displays a screen locally so that the user can perform some protected function, such as enter a Personal ID Number (PIN). Validating an <u>entire computer system</u> to a user so that the user may see a password entry screen does not teach or suggest displaying authentication indicia on the password entry screen so that the user is able to instantly authenticate the screen as valid or invalid.

Second, Pichlmaier does not support the Examiner's assertion that the data word used to authenticate the computer system in Pichlmaier is the claimed authentication indicia. The claimed authentication indicia is stored in secure memory to prevent rogue programs from accessing the authentication indicia. Pichlmaier, on the other hand, relies on randomly generated numbers and enciphering techniques. This evidences the fact that Pichlmaier does not store the code word in secure memory. It is beyond question that random numbers do not require secure memory for storage – they are newly generated at each authentication attempt. Therefore, so, too, are the data words that include the newly generated random number. Moreover, the enciphering techniques necessarily mean that the resultant data word is secure, since according to Pichlmaier, "[o]nly an authorized apparatus is able to decode the code word since only it has the necessary decoding means." *Pichlmaier*, col. 1, ll. 46-48. Thus, the manner in which Pichlmaier generates and sends the data word releases Pichlmaier from having to store the components of that data word (or the data word itself) in secure memory.

Pichlmaier simply does not teach or suggest what the Examiner says it does. Moreover, the Examiner never alleges that the remaining references teach or suggest this aspect, alone or in combination. Therefore, the §103 rejection of claim 1 necessarily fails and must be withdrawn.

Additionally, there is no motivation to combine the references. The Examiner asserts that one skilled in the art would be motivated to modify Pichlmaier to establish a protected channel between the user and a legitimate program as taught by Windows NT and Ozzie. However, this allegation ignores the plain fact that terminating the programs as taught in Windows NT and Ozzie means terminating the very application programs needed by Pichlmaier to function.

Specifically, Pichlmaier requires one or more applications to perform the functions of the disclosed validation process. These include a random number generator to generate the requisite data word, a communication application to communicate the data word with remotely located computers, and an encoding/decoding application to encode/decode the data word. Ozzie explicitly discloses, that when WINDOWS NT receives the CTRL-ALT-DEL key sequence, it "terminates any application programs which are in operation during the password entry sequence." *Ozzie*, col. 1, ll. 46-66. Thus, establishing a protected channel for the Pichlmaier validation process would only terminate the very application programs needed to perform that validation process. As such, establishing a protected channel as asserted by the Examiner would not benefit Pichlmaier, but instead, would render Pichlmaier unusable for its intended purpose. Accordingly, none of the references, alone or in combination, teaches or suggests claim 1 or any of its dependent claims.

The Examiner also rejected claim 11 under §103 for substantially the same reasons as those stated above for claim 1. Claim 11 is an apparatus claim for carrying out the method of claim 1, and thus, recites similar language. Therefore, for reasons similar to those stated above, none of the references teaches or suggests, alone or in combination, claim 11 or any of its remaining dependent claims.

Finally, Applicant has amended the claims to ensure the consistent use of the article "the." The amendments do not add new matter, but simply comply with the Examiner's requirements and address the claim objections on page two of the Office Action.

In light of the amendments and the remarks, Applicant requests that the Examiner withdrawal the objections and allow all pending claims.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: April 5, 2007

Stephen A. Herrera
Registration No.: 47,642

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844
Facsimile: (919) 854-2084